

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed August 10, 2004. In the Office Action, claims 1-20 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses these rejections and requests reconsideration of the allowability of claims 1-20.

Objection of Disclosure

The specification was objected to on the grounds that an article was missing on page 4, line 14 of the specification. More specifically, the phrase "Figure 30 is first embodiment..." should read "Figure 30 is a first embodiment..." Based on the following revisions, Applicant respectfully requests the Examiner to withdraw the outstanding objection.

Rejection Under 35 U.S.C. § 112, Second Paragraph

Claim 12 was rejected under 35 U.S.C. §112, second paragraph as being allegedly indefinite. Applicant has amended claim 12 to include the structural relationship between the memory and the logic to perform the stream cipher. Withdrawal of the §112 rejection is respectfully requested.

Double Patenting Rejection

Claims 1-8, 12-14, and 17-19 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting based on the outstanding claims set forth in a co-pending Application No. 09/864,042). In the event that the Examiner agrees that the claims as amended are in condition for allowance, at that time and as needed, Applicant respectfully offers to submit an executed terminal disclaimer to overcome the obviousness-type double patenting rejection.

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

Rejection Under 35 U.S.C. § 103

A. §103 REJECTION OF CLAIMS 12-18

Claims 12-18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Coppersmith (U.S. Patent No. 6,243,470) in view of Ritter (U.S. Patent No. 5,727,062). Applicant respectfully traverses the rejection.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. See MPEP §2143, p.2100, 124(8th Ed., rev.1, Feb 2003); see also *In Re Fine*, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988). Herein, the combined teachings of the cited references fail to describe or suggest all the claim limitations.

With respect to independent claim 12, the Office Action states that Coppersmith “does not expressly disclose the input data as being segmented into random sized blocks.” See Page 4 of the Office Action. Applicant agrees that Coppersmith offers no such disclosure. However, Applicant disagrees with the Office Action that Ritter provides disclosure of the input data as being segmented into random sized blocks using an encryption key for such segmentation as claimed.

First, based on the teachings of Coppersmith and Ritter, a *prima facie* case of obviousness has not been established because the combined teachings of Coppersmith and Ritter fail to describe or suggest all the claim limitations. The lack of suggestion of all of the claim limitations is due, in part, to the fact that both Coppersmith and Ritter teach away from the claimed limitation of segmenting the input data into *random sized blocks using an encryption key*. It is expressly noted in Coppersmith that “the process of FIG. 3 does not show the user entering particular values to be used for the variables (block size, key size, and the number of rounds) defined for the cipher of the present invention, nor the value to be used for the key. The user will

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

have been prompted to enter these values...." See Col. 7, lines 33-43; Emphasis added. In summary, Coppersmith teaches a cipher processing data blocks of a constant, pre-defined size, and thus, teaches away from segmented into random sized blocks through use of an encryption key.

Ritter teaches blocks of a pre-defined size except for the last block, which may be partially filled. More specifically, column 11, lines 64-67 of Ritter states that "Fig. 1 is an example of an 80-bit block cipher built solely from variable size layers. This makes the cipher easily extendible (in byte-by-byte steps) to arbitrary size, either at design-time or dynamically during operation." This statement, however, indicates that Ritter creates a block cipher to fit the size of an existing length of input data or available data to be encrypted. A block of a variable size comes into effect *only if* the length of the input data is different from some pre-defined block size, and thus, Ritter teaches segmentation where *only the last block is partially filled*. Emphasis added.

As a result, neither Coppersmith nor Ritter, alone or in combination, teaches or suggests performance of a stream cipher operation *on input data segmented into random sized blocks using an encryption key*. Emphasis added. As noted above, Coppersmith teaches blocks having a pre-defined length while Ritter teaches blocks of a pre-defined size except for the last block, which may or may not be partially filled. In effect, Ritter does not teach or even suggest random sized blocks as claimed, but instead teaches pre-defined blocks.

As an example, in the case of Ritter, if N is the number of input data elements to be encrypted, and if C is the block size, then in the case of Ritter, the sequence of block sizes processed are C, C, C, ..., C, x, where $x < C$ if N is not an integral multiple of C. In the case of Coppersmith, the block size is first defined before the encryption begins. For the claimed invention, however, the block sizes used are $n_1, n_2, n_3, n_4, \dots$, which are all different and form a pseudo-random sequence. This sequence is not a static sequence and varies based at least in part on the encryption key to form a different pseudo-random sequence.

Secondly, to provide clarity as to the differences between the claimed invention and the combined teachings of Coppersmith and Ritter, claim 18 has been amended to include the

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

limitation that segmentation of the input data is such that at least three random sized blocks vary in length from a proceeding block. Consideration of these amended claims is respectfully requested.

Therefore, Applicant respectfully submits that neither Coppersmith nor Ritter, alone or in combination, disclose or suggest each and every limitation set forth in independent claims 12 as well as those limitations set forth in dependent claims 13-18. Withdrawal of the outstanding §103(a) rejection is respectfully requested.

B. §103 REJECTION OF CLAIMS 1-3, 9 AND 10

Claims 1-3, 9 and 10 were rejected under 35 U.S.C. §103(a) as being unpatentable over Coppersmith in view of Ritter and Reardon (U.S. Patent No. 6,212,635). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

With respect to independent claim 1, the Office Action states that Coppersmith and Ritter collectively disclose "a first software routine to divide incoming plain text into variable-sized blocks." *See Page 6 of the Office Action.* Applicant respectfully disagrees with the contention as noted above because neither Coppersmith nor Ritter describes or suggest pre-defined block sizes. However, none of these references, including Reardon (USP 6,212,635), suggest variable-sized blocks *with each block varying in size*. Hence, withdrawal of the §103(a) rejection as applied to claim 1 is respectfully requested.

Moreover, as further set forth in dependent claim 2, Applicant respectfully agrees with the Examiner that Coppersmith also does not teach altering the block size based on an encryption key and an internal identifier. *See Page 7 of the Office Action.* However, Applicant disagrees with the Office Action that neither Ritter nor Reardon, alone or in combination, provides any disclosure of forming random-sized blocks of the input data *based on an encryption key, the internal identifier and an output of a first non-linear function.* *Emphasis added.*

Therefore, Applicant respectfully submits that neither Coppersmith, Ritter nor Reardon, alone or in combination, disclose or suggest each of the limitations set forth in independent claim 1 as well as dependent claim 2. Moreover, Applicant respectfully traverses the rejection of

S019.P001X

-10-

WWS/sm

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

dependent claims 3, 9 and 10, but believes that the grounds for traverse need not be enumerated based on the allowability of pending claims 1 and 2. Withdrawal of the outstanding §103(a) rejection is respectfully requested and allowance of claims.

C. §103 REJECTION OF CLAIMS 4-5, 7-8 AND 19-20

Claims 4-5, 7-8 and 19-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Coopersmith in view of Ritter, Reardon and Moskowitz (U.S. Patent No. 5,822,432). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for these claims. However, based on the dependency of claims 4-5, 7-8 on independent claim 1, which is contended to be allowable, Applicant believes that no further discussion as to the grounds for traverse is warranted.

With respect to claim 19, Applicant respectfully traverses their rejection because a *prima facie* case of obviousness has not been satisfied. The reason is that claims 19 was rejected under 35 USC §103(a) based on language allegedly set forth in Moskowitz, which was further used to impermissibly reject dependent claim 7. Applicant submits that the referencing claim language to support the §103 rejection is impermissible because, as the Examiner is aware, a claim "is no measure of what [a patent] discloses." In re Beeno, 226 USPQ 683, 686 (Fed. Cir. 1985). Thus, Applicant respectfully requests the Examiner to specifically point out where in the specification each and every limitation is present in lieu of relying on the claims. Applicant reserves the right to present such arguments in an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 19-20 is respectfully requested.

D. §103 REJECTION OF CLAIM 6

Claim 6 was rejected under 35 U.S.C. §103(a) as being unpatentable over Coopersmith in view of Ritter, Reardon, Moskowitz and Fielder (U.S. Patent No. 5,963,646). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established and the rejection constitutes impermissible hindsight reconstruction in accordance with the Federal Circuit's holding in In re Kotzab, 217 F.3d 1365, 55 U.S.P.Q.2d 1313 (Fed. Cir.2000):

5019.P001X

-11-

WWS/sm

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

Most if not all inventions arise from a combination of old elements. Thus, every element of a claimed invention may often be found in the prior art. See *id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. See *id.* Rather, to establish obviousness based on a combination of the elements disclosed in the prior art, there must be some motivation, suggestion or teaching of the desirability of making specific combination that was made by the applicant.

For this reason, there is no suggestion, motivation or teaching for the desirability of the combination. Withdrawal of the §103(a) rejection is respectfully requested.

E. §103 REJECTION OF CLAIM 11

Claim 11 was rejected under 35 U.S.C. §103(a) as being unpatentable over Coopersmith in view of Ritter, Reardon, and a publication entitled "Cryptography and Network Security (Stallings)". Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established. However, Applicant reserves the right to seek forth the grounds for traversing the rejection in the event that an Appeal is filed in the event that claim 1 is not considered to be in condition for allowance.

Appl. No. 09/895,692
Amdt. Dated: 01/10/2005
Reply to Office Action of 08/10/2004

Conclusion

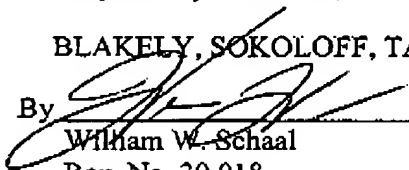
In view of the remarks made above, it is respectfully submitted that pending claims 1-20 define the subject invention over the prior art of record. Thus, Applicant respectfully submits that all the pending claims are in condition for allowance, and such action is earnestly solicited at the earliest possible date. *As mentioned previously in a related application, the Examiner is respectfully requested to contact the undersigned by telephone at the phone number listed below if it is believed that, after review, such claims are still not in condition for allowance. This telephone conference would greatly facilitate the examination of the present application.*

To the extent necessary, a petition for an extension of time under 37 C.F.R. §1.17 is hereby made. Please charge any shortage in fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 01/10/2005

By 
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, PO Box 1450,
Alexandria, VA 22313-1450.

Date: 01/10/2005

FACSIMILE

☒ transmitted by facsimile to the Patent and Trademark Office.


Susan McFarlane
Date: 01/10/2005